

ON SCANNING THE INTERNET OR.... THE CURSE OF IN-THE-CLOUD URL SCANNING



CATALIN COSOI
Head of Online Threats



What Urls Am I Talking About?

Phishing

- Social Media Accounts
- Online Gaming Accounts
- WebMail Accounts
- Financial Institutions

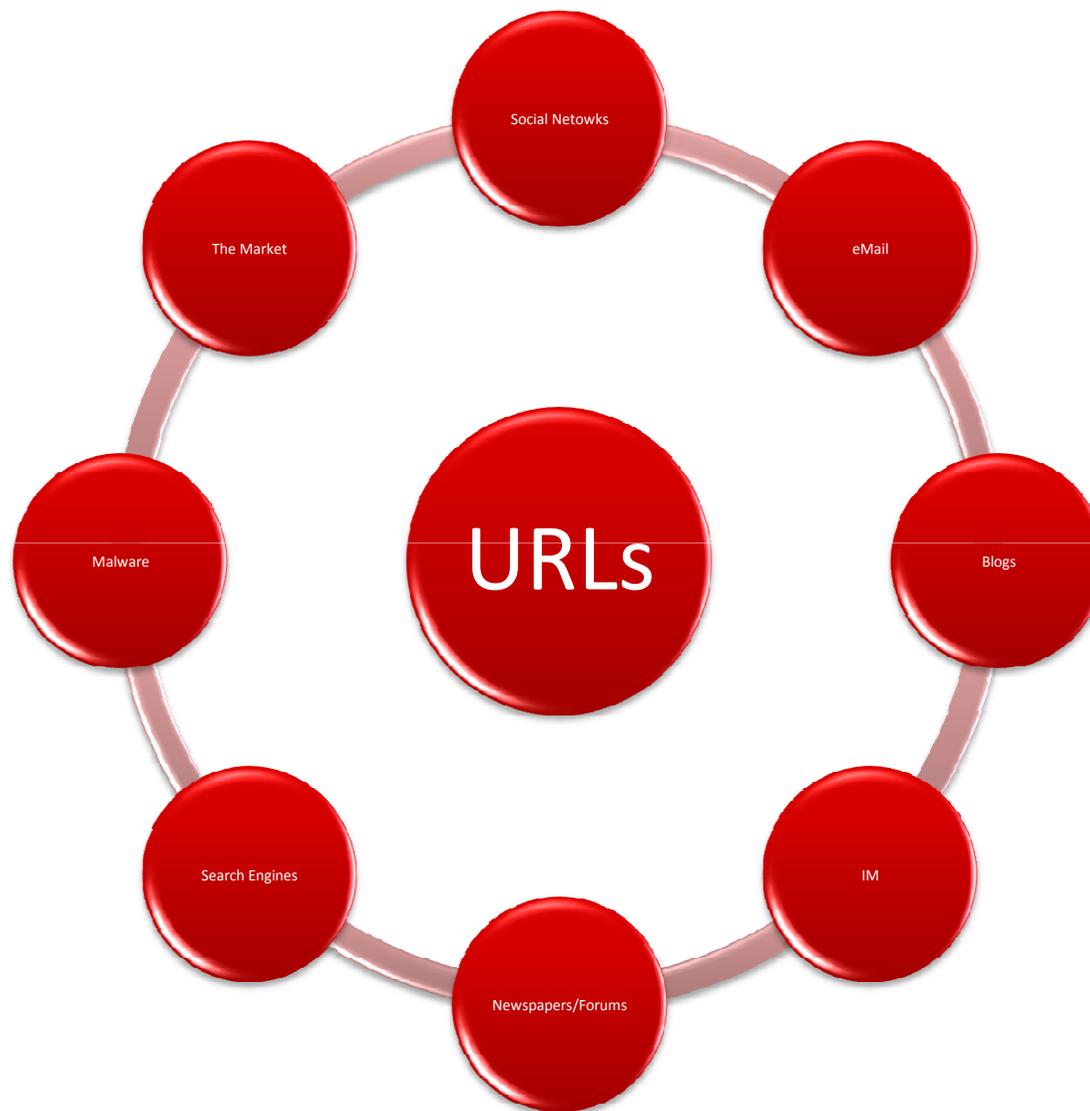
Fraudulent Websites

- Fake Mortgage Websites
- Fake shipping Websites
- Fake (cheap) pills
- Actually all scams go here

Malware

- Old school Malware
- Fake AVS
- etc

Where Do Urls Come From?



Contents

- Short intro into the cloud
- Pros and Cons of cloud computing
- And some more pros and cons
- Some of our stories
- Obviously, some conclusions

What is the Cloud? Where is the Cloud?

- Cloud Computing in the security industry has multiple definitions and several approaches.
- Security in the cloud means:
 - URL scanning
 - AV scanning
 - Spam scanning
 - RBL
 - And more



Current Status of the Cloud Paradigm

- Pro Cloud
- Against Cloud
- A hybrid approach is better



We are here!

Why Should We Go for it? (the Strengths)

- No versioning (no large product updates)
- Low resource consumption
- Higher speed
- Not OS dependant
- Not hardware dependant
- Instant access to updates
- New technologies available like outbreak detection or statistics based algorithms
- Sometimes.... It is also cheaper

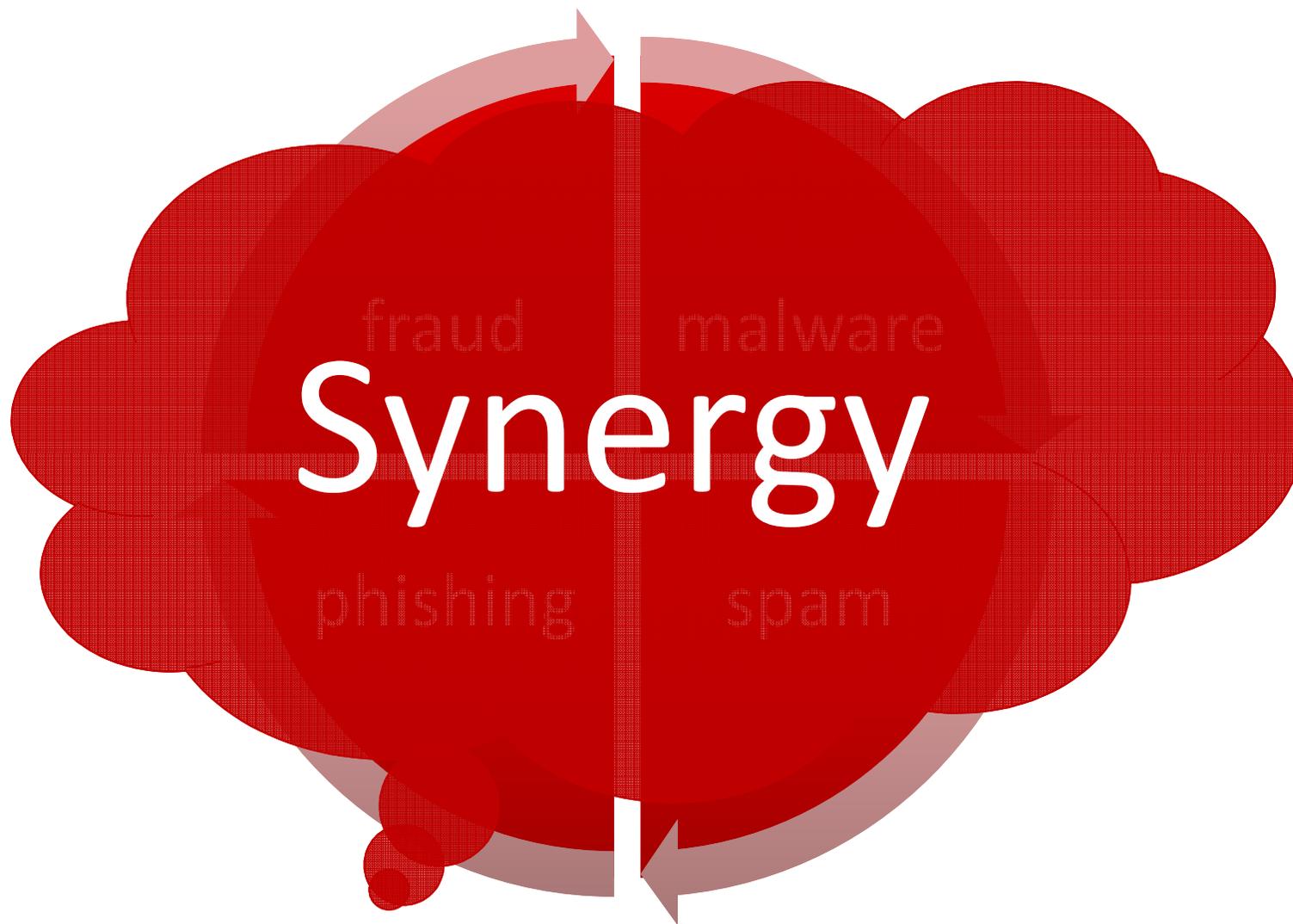


Why We Shouldn't? (the Weaknesses)

- No internet connection means no cloud
- Susceptible to DDOS attacks
- Resource Consumption just moved in the cloud.
It didn't vanished!
- Connection spikes can cause false negatives (or, even DDOS->self)
- Instant updates can also mean instant faulty updates
- Data center failure means no detection (the cleaning lady effect)



So What Does Exactly Cloud Offer Me?



What Else Can Cloud Offer?

- Opens the door to a new set of
 - Applications
 - Devices
 - Operating systems



share links
Saf.li
Shortens your links ✓
Checks them for viruses ✓
Checks them for phishing ✓

Safe short links anyone ?

Share Saf.li

Step 1

Enter your long URL.

Step 2

Click the button to have your link checked for malware by BitDefender and make sure the web page is not set up to steal users personal data.

Step 3

Share your link or post it to your favorite Social Media Site.

[Tell me more about Saf.li](#)



Want to integrate the Saf.li service into your website or application? [Click here to check out our SDK](#)



Send us your suggestions for improving Saf.li, by email at safli@bitdefender.com

Made safe by
bitdefender

more

Provide Help For the Bloggers (WP Users and More)

 **BitDefender Anti-Spam** Help ▾

[Logging](#) | [Spam Settings](#) | [Stats](#) | [Feedback](#)

Plugin revision: 12645

An experimental AntiSpam solution for WordPress based blogs

This experimental WordPress Plugin will work with the API on BitDefender's cloud based scanning servers to ensure no spam hits your blog. This version of BitDefender AntiSpam for WordPress was released as PREVIEW and we welcome any form of feedback or suggestions. Please tell us what you think about: detection rate (both undetected spam and false positives), the overall look&feel when installing or working with the plugin and basically any other information (including flames) you feel would help us improve this project.

BitDefender AntiSpam for WordPress is released by BitDefender's Innovation and Technology team and is Free to use. For feedback, flames and suggestions you can contact us at asblog@labs.bitdefender.com

BitDefender Client ID

Enter your e-mail address to identify yourself to the BitDefender AntiSpam API
This identifies your blog to the Bitdefender servers hosting the scanning services.

Blog language

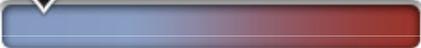


Offer Support to Facebook Users



PROFILE

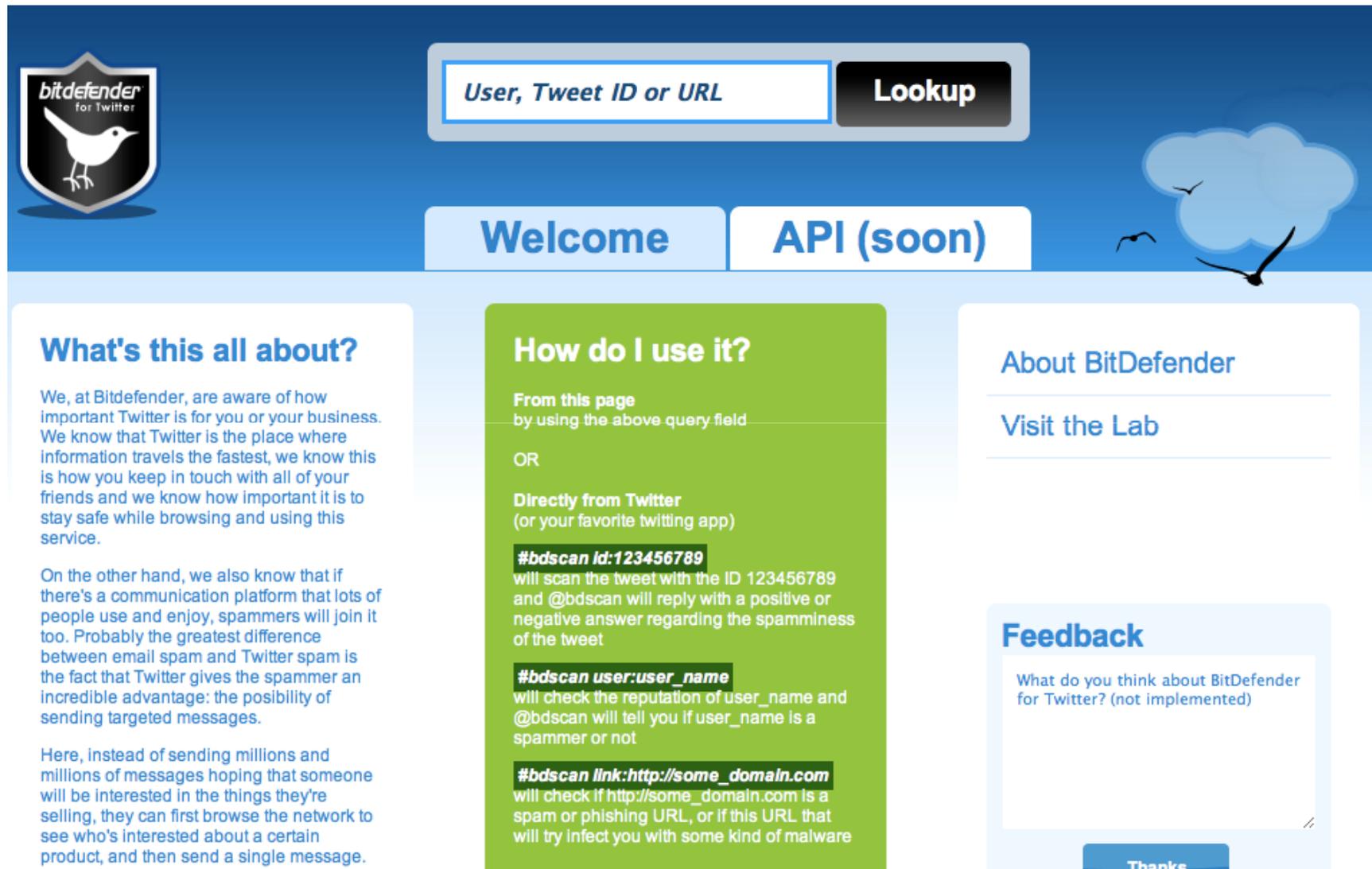
BitDefender scans your profile to determine what information is visible by people and applications that you are not in contact with. Due to the way Facebook shares information, unless you specifically set it private, some information will be public. By default some of your profile informations are public and another bit is visible by Friends of your Friends. BitDefender tells you what other people can learn about you trough your profile. To protect your online privacy, we suggest you verify your [Privacy Settings](#)

| PROFILE INFO | STATISTICS | PRIVACY LEVEL |
|---|---|--|
|  |  2085 SCANNED ITEMS |   |
| NAME: Catalin |  1204 LINKS | THE FOLLOWING ITEMS, REQUEST ATTENTION:  FEED  POSTS  LINKS |
| SURNAME: Cosoi |  0 INFECTED | |
| E-MAIL: | ON DEMAND SCAN SCAN NOW | |

WALL AND INBOX SANITY

BitDefender checks your information feeds (home, inbox, outbox) for spam messages using our sophisticated scanning technology. This allows us to warn you in case a message in your feed or inbox is malicious or if it contains links to malware. You can then delete those messages. As a general rule, be careful when following links on Facebook to unknown sites even if they originate from your friends

Assist Twitter Users



The screenshot shows the BitDefender for Twitter website. At the top left is the BitDefender logo. In the center, there is a search bar with the placeholder text "User, Tweet ID or URL" and a "Lookup" button. Below the search bar are two tabs: "Welcome" and "API (soon)". The main content area is divided into three columns. The left column is titled "What's this all about?" and contains three paragraphs of text. The middle column is titled "How do I use it?" and contains three sections: "From this page", "Directly from Twitter", and three examples of query strings. The right column is titled "About BitDefender" and "Visit the Lab". At the bottom right, there is a "Feedback" section with a text input field and a "Thanks" button.

bitdefender
for Twitter

User, Tweet ID or URL **Lookup**

Welcome API (soon)

What's this all about?

We, at Bitdefender, are aware of how important Twitter is for you or your business. We know that Twitter is the place where information travels the fastest, we know this is how you keep in touch with all of your friends and we know how important it is to stay safe while browsing and using this service.

On the other hand, we also know that if there's a communication platform that lots of people use and enjoy, spammers will join it too. Probably the greatest difference between email spam and Twitter spam is the fact that Twitter gives the spammer an incredible advantage: the possibility of sending targeted messages.

Here, instead of sending millions and millions of messages hoping that someone will be interested in the things they're selling, they can first browse the network to see who's interested about a certain product, and then send a single message.

How do I use it?

From this page
by using the above query field

OR

Directly from Twitter
(or your favorite twitting app)

#bdscan id:123456789
will scan the tweet with the ID 123456789 and @bdscan will reply with a positive or negative answer regarding the spamminess of the tweet

#bdscan user:user_name
will check the reputation of user_name and @bdscan will tell you if user_name is a spammer or not

#bdscan lnk:http://some_domain.com
will check if http://some_domain.com is a spam or phishing URL, or if this URL that will try infect you with some kind of malware

About BitDefender

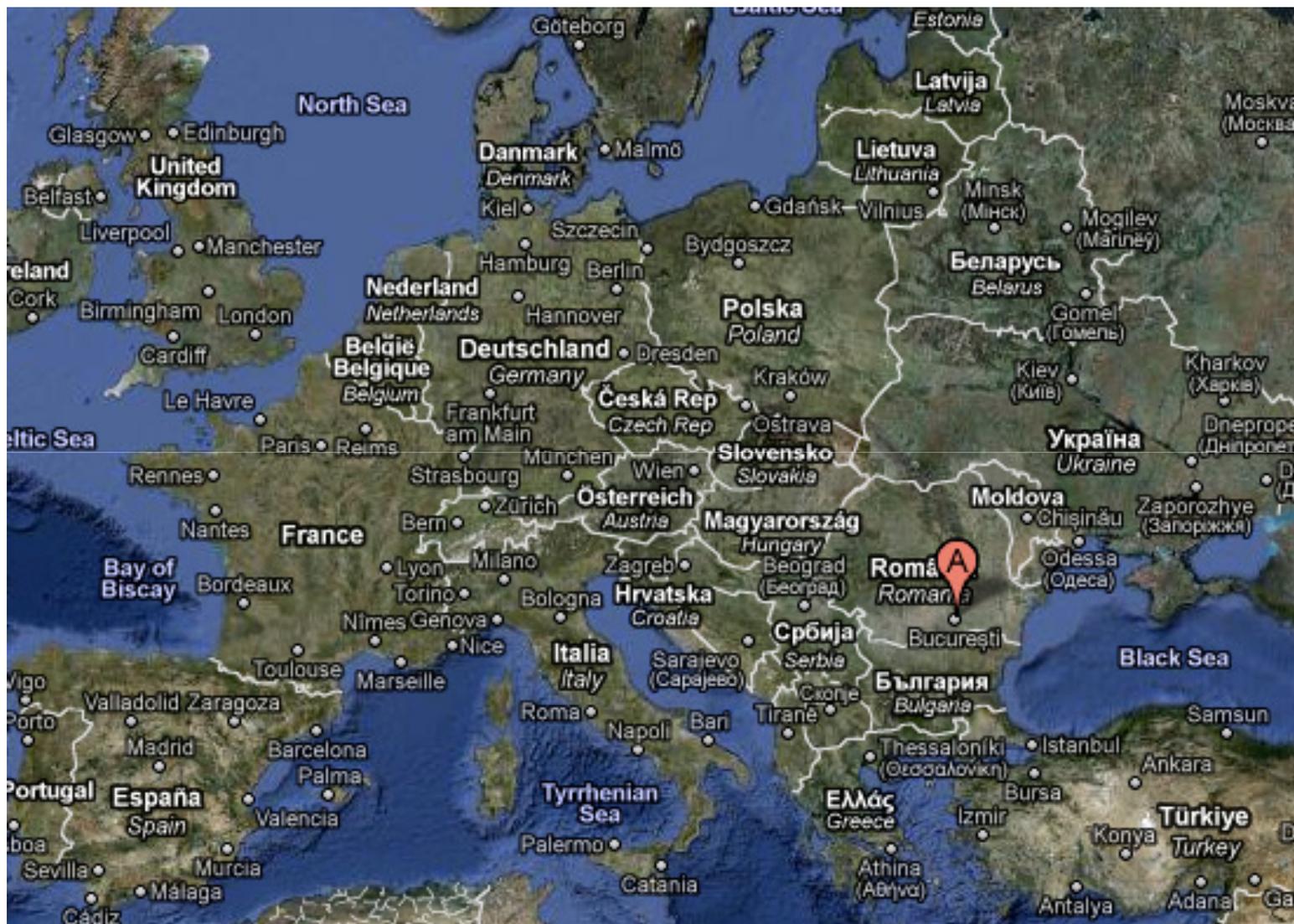
Visit the Lab

Feedback

What do you think about BitDefender for Twitter? (not implemented)

Thanks

geolP Based Attacks



You Have to Login First!

- HTTPS webpages
- Sites where you have to login
- Sites that require user interaction



Size Does Matter!

- Several sources of URLs means an extremely large number of URLs
- Several clients that query the cloud means a massive number of links that have to be analyzed
- Links have various statuses (clean, infected, phishing, fraud) which change dynamically
- So, one has to move fast...

Lies, Damned Lies and Statistics

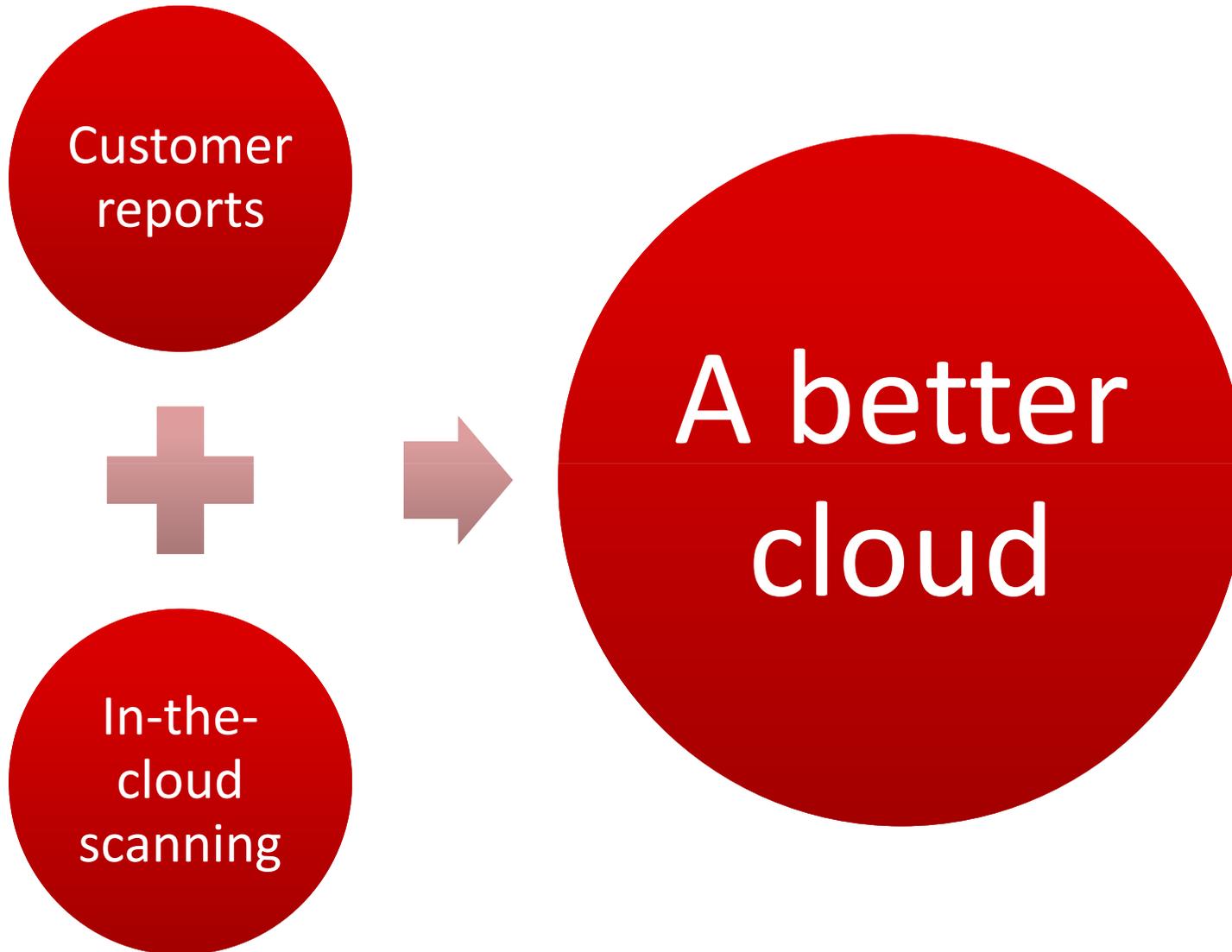
- Targeted attacks stay under the
- Slow spreading malware too



Not Everyone Presses the “Like” Button

- Not everybody likes us
 - Website owners
 - ISPs
 - Maybe even social networks?
 - And hopefully the bad guys

Enhancing the Cloud



Conclusions

- We believe that a hybrid approach is best
- The cloud should be used as another filtering method and not as a universal solution
- Not only there should be a hybrid approach, but also these techniques have to be interconnected
- Although it looks quite easy in theory, creating and maintaining a cloud architecture is not an easy process



A PENNY FOR YOUR THOUGHTS?!?

Alexandru Catalin COSOI
Head of Online Threats Lab
eMail: acosoi@bitdefender.com

